



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/819,359	03/28/2001	Satoshi Hada	JP919990280US1	3306

23389 7590 06/16/2005

SCULLY SCOTT MURPHY & PRESSER, PC
400 GARDEN CITY PLAZA
SUITE 300
GARDEN CITY, NY 11530

EXAMINER

POLTORAK, PIOTR

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 06/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/819,359

Applicant(s)

HADA, SATOSHI

Examiner

Peter Poltorak

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 March 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. The Amendment, and remarks therein, received on 3/24/2005 have been entered and carefully considered.
2. The Amendment introduces amended claims 1 and 7-17, and adds new claims 18-23.
3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.

Response to Amendment

4. Applicant's arguments have been carefully considered but they were not found persuasive.
5. As per claims 1, 7-10 and 12 applicant amended the claim language so instead of alternative steps, only one set of steps is performed. As a result, applicant argues the previous Office Action did not address claims limitation.
6. This Office Action addresses the current (alternative) step below.
7. Claims 1-23 have been examined.

Claim Objections

8. Claim 7 is objected to because of the following informalities: two "cryptogram" words appear one after another. One of the words should be deleted. Appropriate correction is required.
9. Claims 1-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Schneier (Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source*

Code in C", 2nd edition, 1996 ISBN: 0471128457) in view of Trostle (U.S. Patent No. 6718467).

10. As per claims 1-6 *Schneier* teaches *Diffie-Hellman's* key-exchange algorithm (*Schneier pg. 513*) which covers the limitation of claim 1 reading on calculating

Prover (Alice)	Verifier (Bob)
$A = F(g, a)$	$B = F(g, b)$
$F(B, a)$	$X = F(A, b)$

11. *Schneier* teaches that $F(Y, x) = FX(X, y)$. He also teaches *Schnorr's* authentication protocol which reads on the limitation of claim 1 disclosed on pg. 1 lines 23 – pg. 2 line 3, in which data required for verifying the equation is sent to the opposite communication party. In addition *Schneier* teaches ciphertext-only cryptanalysis attacks (*Schneier pg. 5 last § – pg. 6 first §*).
12. *Schneier* teaches implicitly that computers are used to implement the algorithms (*pg. 22 and 23, The Purpose of Protocols and The Players sections*).
13. *Schneier* does not teach transmitting X for verification and determining whether $X = F(B, a)$, and does not teach determining that said relation between the prover computer and the verifier computer is correct.
14. *Trostle* teaches mutual authentication (*Trostle col. 7 lines 19-33*).
15. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to extend the *Diffie-Hellman's* algorithm by transmitting X for verification, and determining whether $X = F(B, a)$ is established. One of ordinary skill in the art

Art Unit: 2134

would have been motivated to perform such a modification in order to prevent ciphertext-only attacks.

16. It would also have been obvious to one of ordinary skill in the art to authenticate the prover to the verifier in order to determine that the relation between the prover computer and verifier computer is correct (*mutual authentication*) employing the reverse transaction. One of ordinary skill in the art would have been motivated to perform such a modification in order to validate communicating parties to lower security risks.

17. At the same time, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement an additional verification that the prover is the entity, which it claims to be (*verification such as Schnorr's, Schneier last § pg. 510 – § 3 pg. 511*) for benefit of increase level of security.

18. Claims 7-14 and 16-17 are substantially equivalent to claims 1-7; therefore claims 7-14 and 16-17 are similarly rejected.

19. Claims 18-23 show essentially the same steps as cited in previous claims, e.g. claim 1. Even though the notation is not identical and verification is achieved employing different character set in light of employed public key cryptography the steps introduced in claims 18-23 are simply obvious variation of steps seen in the previous claims (*e.g. claim 1*). One of ordinary skill in the art would have been motivated to perform such a modification to actuate such security measures.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571)272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Signature
6/9/05
Date

David Y. Jung
Primary Examiner

A.U. 2134
